77 Rec'd PCT/PTO 23 NOV 2001

orm PTO-1390 21705.P01	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER P21705
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/926594

NTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
CT/KR00/00875	August 9, 2000	April 14, 2000

TLE OF INVENTION

ETHOD AND APPARATUS FOR PROTECTING FILE SYSTEM BASED ON DIGITAL SIGNATURE CERTIFICATE

PPLICANT(S) FOR DO/EO/US

ou-Jin EUN, Ki-Yoong HONG, Min-Goo LEE, and Jae-Myung KIM

pplicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

. X This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.

. ___ This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.

. X This is an express request to promptly begin national examination procedures (35 U.S.C. 371(f)).

X The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).

X A copy of the International Application as filed (35 U.S.C. 371(c)(2))
a. X is attached hereto (required only if not communicated by the International Bureau).
b. X has been communicated by the International Bureau.
c. ___ is not required, as the application was filed in the United States Receiving Office (RO/US).

___ An English language translation of the International Application as filed (35 U.S.C. 371 (c)(2)).

___ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
a. ___ are attached hereto (required only if not communicated by the International Bureau).
b. ___ have been communicated by the International Bureau.
c. ___ have not been made; however, the time limit for making such amendments has NOT expired.
d. ___ have not been made and will not be made.

___ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3))

X An oath or declaration of the inventor(s) (35 U.S.C. .371(c)(4)).
"Executed"

___ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (U.S.C. 371(c)(5)).

ms 11 to 16 below concern other document(s) or information included:

Assignee: SECUVE CO., LTD. of Kyoungki-do, Republic of KOREA

___ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

X An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

___ A FIRST preliminary amendment.
___ A SECOND or SUBSEQUENT preliminary amendment.

___ A substitute specification.

___ A change of power of attorney and/or address letter.

X Figure of Drawing to be published ____1____

X Other items or information:
Cover Sheet and International Application as published
PCT/RO/101-PCT Request.
PCT/IPEA/401.
PCT/IB/308.
PCT/ISA/210.
Claim of Priority.

JC13 Rec'd PCT/PTO 23 NOV 2001

U.S. APPLICATION NO. (If known, see 37 CFR 5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/926594	PCT/KR00/00875	P21705

0. X The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search report has been prepared by the EPO or JPO. . . . . $ 890.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482). . . . . $ 710.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO(37 CFR 1.445(a)(2). . . . . $ 740.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO. $1,040.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4). . . . . $ 100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$1,040.00	
archarge of $130.00 for furnishing the oath or declaration later than ___ 20 ___ 30 onths from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed		Number Extra	RATE		
otal Claims	33	- 20 =	13	X $18.00	$234.00	
dependent Claims	3	- 3 =	0	X $84.00	$0.00	
ultiple dependent claim(s) (if applicable)				+ $280.00	$0.00	
			TOTAL OF ABOVE CALCULATIONS =		$1274.00	
Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by ½.					$637.00	
			SUBTOTAL =		$637.00	
ocessing fee of $130.00 for furnishing the English translation later than ___ 20 ___ 30 onths from the earliest claimed priority date (37 CFR 1.492(f)). +						
tension of Time fee in the amount of $						
			TOTAL NATIONAL FEE =		$637.00	
e for recording the enclosed assignment (37 CFR 1.21(h). The assignment must be ompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +					$40.00	
			TOTAL FEES ENCLOSED =		$677.00	
				Amount to be refunded	$	
				Charged	$	

X A check in the amount of $677.00 to cover the above fees is enclosed.

___ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees.

X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 19-0089.

TE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and nted to restore the application to pending status.

ND ALL CORRESPONDENCE TO **CUSTOMER NO. 7055**
THE PRESENT ADDRESS OF:
ce H. Bernstein
EENBLUM & BERNSTEIN, P.L.C.
1 Roland Clarke Place
ton, VA 20191
3) 716-1191

07055
PATENT TRADEMARK OFFICE

Leslie J. Paperner Reg. No.
SIGNATURE
Bruce H. Bernstein 33,329
NAME

29,027
REGISTRATION NUMBER

13/prts

METHOD AND APPARATUS FOR PROTECTING FILE SYSTEM BASED ON DIGITAL SIGNATURE CERTIFICATE

Field of the Invention

The present invention relates to a method and apparatus for protecting a file system; and, more particularly to a method and apparatus for protecting a file system based on a digital signature certificate in a computer system.

Prior Art of the Invention

In a conventional computer system, in order to protect a sever computer, an access control method or one-time password is used.

The computer system using the access control method permits a certain user to access only predetermined services or network addresses. In other words, the computer system prevents a user having no access authority from accessing except for the predetermined service or the predetermined network address.

A general password used for identifying a user is registered once and continually used until another password is registered. In order to prevent a malicious user from making a fraudulent use of the password, the one-time password is used. The one-time password means a password that is used only one time.

However, since a hacking method which a malicious hacker can obtain an authority of a system security manager or a general user by only accessing the predetermined service or network address has been introduced, interception of access to a certain service or network can not substantially protect the file system from the malicious hacker trying to forge or to alter the file system, e.g., a home page.

Various hacking techniques make partial security function of the one-time password powerless.

The problems of the access control method and one-time password result from a computer operating system that provides the conventional security technique implemented in application program, user or network level.

Summary of the Invention

Therefore, it is an object of the invention is to provide a method and apparatus for protecting a file system.

It is another object of the invention is to provide a safe and stable computer system.

In accordance with an aspect of the present invention, there is provided a method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the method comprising the steps of: a) generating system security manager's digital signature keys and system security manager's certificate; b) storing system security manager's certificate

onto a security kernel when installing an operating system on a server computer; c) generating second digital signature keys and user's certificate; d) setting an access authority of the file system; e) identifying a user through a digital signature based authentication when the user tries to access the file system; and f) giving the user the access authority for the file in accordance with identification result.

In accordance with another aspect of the present invention, there is provided an apparatus for protecting a file system in a computer system, wherein a user having a file access authority can access the file system in the computer system, the apparatus comprising: means for generating system security manager's digital signature keys and system security manager's certificate; means for storing system security manager's certificate onto a security kernel when installing an operating system on a server computer; means for generating user's digital signature keys and user's certificate; means for setting an access authority of the file system; means for identifying a user through a digital signature authentication method when the user tries to access the file system; and means for giving the user the access authority for the file in accordance with identification result.

Brief Description of the Drawings

The above and other objects and features of the instant invention will become apparent from the following description

of preferred embodiments taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a diagram of a computer system to which the present invention is applied;

Fig. 2 is a detailed diagram of a server computer in accordance with the present invention;

Fig. 3 is a detailed diagram of the security kernel of Fig. 2;

Fig. 4 is a detailed diagram of the certificate storage of Fig. 2;

Fig. 5 is a detailed diagram of the process security information storage in the security kernel of Fig. 3;

Fig. 6 is a detailed diagram of a file security information storage in the security kernel of Fig.3;

Fig. 7 is a flow chart illustrating a method for operating a file protecting method in accordance with the present invention;

Fig. 8 is a flow chart illustrating a method for installing the file protecting method on a server computer in accordance with the present invention;

Fig. 9 is a flow chart illustrating a method for operating the file protecting method in accordance with the present invention;

Fig. 10 is a flow chart illustrating a digital signature based authentication in accordance with the present invention;

Fig. 11 is a flow chart illustrating a method for registering/deleting a user in accordance with the present

invention;

Fig. 12 is a flow chart illustrating a method for setting an access authority of a file in accordance with the present invention; and

Fig. 13 is a flow chart illustrating a method for processing a file.

Preferred Embodiments of the Invention

Hereinafter, preferred embodiments of the present invention will be described in detail with reference to the accompanying drawings.

Fig. 1 is a diagram of a computer system to which the present invention is applied.

The computer system includes a sever computer 110 and computers 120, 140 and 150 for a system security manager, a user at a remote distance and a user at a short distance from the server computer 110.

Each of computers 120, 140 and 150 has a storage device such like a floppy diskette 124, 144 and 154 and a smart card 126, 146 and 156. The sever computer 110 and the computers 120, 140 and 150 are connected to each other in direct or through a computer network 130.

The system security manager manages the sever computer 110 and users of the sever computers 110 after obtaining authentication based on digital signature.

The user 150 at a short distance from the sever computer

110 can access a part of files after being identified based on digital signature. The part of files are allowed to be accessed by the user. The system security manager sets an access authority of a file and an access authority of a user.

The user 140 at a remote distance from the sever computer 110 can access a part of files allowed to be accessed by the user after being identified based on digital signature generated by communications through a computer network.

Fig. 2 is a detailed diagram of a server computer in accordance with the present invention.

The server computer includes a plurality of elements in a user level, a kernel level and hardware level.

The user level of the server computer includes a certificate storage block 212, a security management module 214, a security library 216, and a library 218.

The security management module 214 generates a pair of encryption key used for generating a digital signature value of the system security manager or the user at a short/remote distance. The pair of encryption keys includes a secret key and a public key. Also, the security management module 214 issues a certificate based on the encryption keys and the digital signature value.

The kernel level of the server computer includes a system call interface block 232, a file subsystem 234, a process control subsystem 236, a security kernel 238, a device driver 240 and a hardware controller 242.

The system call interface block 232 interfaces the

elements in the user level with the elements of the kernel level.

The security kernel 238 verifies the digital signature, sets and inquires the access authority of the file. Also, the security kernel 238 controls an access of the file.

The hardware level of the server computer includes a driver controller, a hard disk driver, a floppy disk driver, a smart card driver, a Universal Serial Bus (USB) driver and a network driver.

These elements in the hardware level are well known to those skilled in the art. Accordingly, detailed description on these elements will be skipped in this specification.

Fig. 3 is a detailed diagram of the security kernel of Fig. 2.

The security kernel includes an access authority control block 302, a digital signature verification block 304, an access authority setting/inquiry block 306, a security rule setting/inquiry block 308, a file system access authority decision block 310, a system security manager certificate storage 312, a process security information storage 314, a security rule storage 316 and a file system security information storage 318.

Security information related to the process is stored on the process security information storage 314, security rule information is stored on a security rule storage 316 and security information related to the file system is stored on a file system security information storage 318.

The access authority control block 302 controls the access authority setting/inquiry block 306, the security rule setting/inquiry block 308 and the file system access authority decision block 310.

The access authority setting/inquiry block 306 includes a process security information storage 320 and a file system security information setting/inquiry block 322. If a user trying to access a file is identified in the access authority control block 302, information on the process security information storage 314 is set by the process security information setting/inquiry block 320.

The file system security information setting/inquiry block 322 sets and inquires the file system security information storage 318.

The security rule setting/inquiry block 308 sets and inquires the security rules stored on the security rule storage 316.

The security rule setting/inquiry block 308 communicates with the access authority setting/inquiry block 306 and the file system access authority decision block 310 and provides information necessary for an access control based on the security rules stored on the security rule storage 316.

The file system access authority decision block 310 compares information stored on the process security information storage 314 with the file system security information stored on the file system security information storage 318. The file system access authority decision block

310 determines whether an access authority is provided to the user based on the security rule stored on the security rule storage.

Fig. 4 is a detailed diagram of the certificate storage of Fig. 2.

The certificate storage 212 includes a plurality of certificates. The certificates include a user identification (ID) 410, 430 and 450 and a user certificate 420, 440 and 460. Each of the user identifications (ID) 410 represents the user possessing each of the user certificates 420. The pair of certificate is added, deleted or searched in accordance with a control signal from the security management module 214 of Fig. 2.

The user certificate 420 includes a system security manager identification (SM ID) 421, a user identification 422, an access authority identification (ID) 423, an access valid date 424, a public key 425, an issue time 426, a certificate valid date 427 and a digital signature value 428.

The system security manager identification 421 represents a system security manager SM who issues the user certificate.

The user identification 422 represents a user possessing the user certificate 420.

The access authority identification (ID) 423 represents an access authority of the user.

The access valid date 424 represents a valid time. The user can access the file system by the valid time.

The public key 425 is used for verifying a digital

signature of a user. The issue time 426 represents a time on which the user certificate is issued.

The digital-signature value 428 represents a value digital-signed of the user certificate except the digital signature value 428 by using a secret key of the system security manager.

Fig. 5 is a detailed diagram of the process security information storage in the security kernel in Fig. 3.

In the process security information storage 314, a plurality of process identifications (ID) 510, system security manager flags 512 and access authority identifications (ID) 514 are stored. The process security information storage 314 searches the process identification 510 to be accessed. After finding the process ID, the process security information storage 314 sets or inquires a corresponding system security manager flag or access authority identification in accordance with a control signal from the process security information setting/inquiry block 320, the file system security information setting/inquiry block 322 or the file system access authority decision block 310.

Each of the process IDs 510 represents a process executed by the user.

Each of the system security manager flags 512 represents a system security manager by which a process is executed. Each of the access authority ID 514 represents an access authority permitted to the process.

Fig. 6 is a detailed diagram of a file system security

information storage in the security kernel. The file system security information storage 318 of Fig. 3 includes a file identification (ID) 602 and an access authority identification (ID) 604. The access authority identification (ID) 604 corresponding to the file identification (ID) 602 is set or inquired in accordance with a control signal the file system security information setting/inquiry block 322 or the file system access authority decision block 310.

The file identification (ID) 602 represents an identification used for identifying a file. The access authority identification (ID) 604 represents an access authority of the user allowed to access the file.

Fig. 7 is a flow chart illustrating a method for operating a file protecting method in accordance with the present invention.

First, an install process for setting a system security manager is performed at step 702. Next, an operating process is performed at step 704. In the operating process, a user registering/deleting process, a file access authority setting process or a file accessing process is performed after user authentication. Then, it is determined whether the file protecting method is terminated or not at step 706. If the method is not terminated, the process continues to step 704. If so, the method ends.

Fig. 8 is a flow chart illustrating a method for installing the file protecting method on a computer in accordance with the present invention.

First, the server computer generates a pair of keys for the system security manager, a public key PK_SM and a secret key SK_SM at step 802.

The sever computer generates a certificate for the system security manager at step 804. System security manager's access authority ACID_SM and system security manager's public key PK_SM are digital-signed by system security manager's secret key SK_SM, thereby generating the certificate for the system security manager.

The system security manager encrypts his/her secret key SK_SM and stores the encrypted secret key onto a memory device, e.g., a smart card or a floppy disk at step 806.

The system security manager stores his/her certificate CERT_SM onto a memory device, e.g., a smart card or a floppy disk at step 808. Also, the system security manager stores his/her certificate CERT_SM onto the system security manager certificate storage 312 in the security kernel 238 at step 810.

The install process is terminated and returns to step 704.

Fig. 9 is a flow chart illustrating a method for operating the file protecting method in accordance with the present invention.

First, the server computer verifies a system security manager or a user trying to access itself by using digital signature based authentication at step 902. It is determined whether authentication result is success or fail at step 904.

If the authentication result is fail, the process terminates.

If the authentication result is success, the process goes to step 906 to load system security manager's certificate stored onto the system security manager certificate storage 312 and extracts system security manager's access authority ACID_SM from system security manager's certificate. And then, the process continues to step 908 to determine whether user's access authority ACID_U is equal to system security manager's access authority ACID_SM.

If user's access authority ACID_U is equal to system security manager's access authority ACID_SM, system security manager's access authority is applied to an access authority of a user process ACID_UP at step 910. The user process having system security manager's access authority ACID_SM selects and executes one of a user registering/deleting process, a file system access authority setting process and a file access process at steps 914, 916, 918 and 920.

If not, user's access authority ACID_U is applied to an access authority ACID_UP of a user process at step 912. The user process executes a file access process at step 920.

Then, the process returns to step 706.

Fig. 10 is a flow chart illustrating a digital signature based authentication process in accordance with the present invention.

The server computer generates a random number R at step 1002. The user generates a digital-signature value X to the random number R by using its secret key at step 1004. The server computer loads system security manager's certificate

CERT_SM stored in the system security manager certificate storage in the security kernel 238 at step 1006. The server computer extracts the public key PK_SM of the system security manager from the certificate CERT_SM of the system security manager, the certificate CERT_SM being stored on the security kernel, at step 1008.

The certificate CERT_U of the user is verified by the security kernel 238 at step 1010. Then, it is determined whether verification result is success or fail at step 1012. If the verification result is fail, the process stores the verification result as a fail and terminates.

If the verification result is success, the security kernel extracts the public key PK_U and the access authority ACID_U of the user from the certificate CERT_U of the user at step 1014. After extracting the public key and the access authority for the client user, the security kernel verifies the digital signature value X to the random number R at step 1016. If an authentication result is success, the process stores the authentication result as a success and returns the access authority ACID_U of the user to the step 904 in order to be used at step 908.

Fig. 11 is a flow chart illustrating the user registering/deleting process in accordance with the present invention.

First, it is determined whether the access authority ACID_UP of the user process is equal to that ACID_SM of the system security manager at step 1102. If the access authority

ACID_UP of the user process is not equal to that ACID_SM of the system security manager, the process terminates and returns.

If the access authority ACID_UP of the user process is equal to that ACID_SM of the system security manager, the process continues the step 1104 to select a user registering process or a user deleting process.

If the user deleting process is selected, the user process having the access authority of the system security manager deletes the registered user at step 1106.

If the user registering process is selected, the user process having the access authority of the system security manager gives an access authority to a new user at step 1110. The user process generates a public key PK_U and a secret key SK_U for the new user at step 1112.

The system security manager encrypts the access authority and the public key for the new user by using its secret key, thereby generating a certificate CERT_U for the new user at step 1114. The new user encrypts its secret key and stores the encrypted secret key onto a memory device, e.g., a smart card or a floppy diskette at step 1116. The new user stores its certificate CERT_U onto the memory at step 1118. Then, it is determined whether the process is terminated or not at step 1120. If the process is terminated, the process returns. If not, the process goes to the step 1104 to select a user registering process or a user deleting process.

Fig. 12 is a flow chart illustrating a file access

authority setting process in accordance with the present invention.

First, it is determined whether the access authority ACID_UP of the user process is equal to that ACID_SM of the system security manager at step 1202. If the access authority ACID_UP of the user process is equal to that ACID_SM of the system security manager, the system security manager selects a file of which access authority is to be set at step 1204. If not, the process terminates.

The system security manager selects users who are allowed to access the file at step 1204. The security kernel sets an access authority ACID_F of the file selected at the step 1204 as the access authority ACID_U of the user selected at the step 1206 at step 1208. Then, it is determined whether the process is terminated at step 1210. If the server computer selects termination, the process terminates. If not, the process continues to the step 1204.

Fig. 13 is a flow chart illustrating a method for processing a file.

The security kernel obtains a file to be accessed at step 1302. The security kernel compares the access authority ACID_UP of the user process trying to access the file with the access authority ACID_SM of the system security manager at step 1304.

If the access authority ACID_UP of the user process is equal to that ACID_SM of the system security manager, the server computer permits the user process to access the file F

at step 1306. Then, it is determined whether the process is terminated. If the sever computer selects termination, the process terminates. If not, the process continues to the step 1302.

If the access authority of the client user process is not equal to that of the system security manager, the process goes to step 1308 to determine whether the access authority of the user process ACID_UP is equal to that ACID_UP of the user at step 1308. If not, the process terminates.

If the access authority ACID_UP of the user process is equal to that ACID_SM of the user, it is determined whether the access authority ACID_UP of the user process is equal to that ACID_F of the file F at step 1310. If not, the process terminates.

If the access authority ACID_UP of the user process is equal to that ACID_F of the file F, the server computer permits the user process to access the file at step 1312. Then, it is determined whether the process is terminated. If the server computer selects termination, the process terminates. If not, the process continues to the step 1302.

The file protecting system in accordance with the present invention stores the certificate of the system security manager onto the security kernel in the kernel level at system install process. Also, the digital signature based authentication, a file access authority setting process and a file access process are performed in the kernel level not in the user level. Accordingly, the file protecting system can

fundamentally prevents the file system from being forged or altered.

Therefore, the file protecting system in accordance with the present invention provides a stable and reliable file system. For example, the file protecting system in accordance with the present invention can protect a web server system operating a homepage from a hacking.

Although the preferred embodiments of the invention have been disclosed for illustrative purpose, those skilled in the art will be appreciate that various modifications, additions and substitutions are possible, without departing from the scope and spirit of the invention as disclosed in the accompanying claims.

What is claimed is:

1. A method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the method comprising the steps of:

a) generating system security manager's digital signature keys and system security manager's certificate;

b) storing system security manager's certificate onto a security kernel when installing an operating system on a server computer;

c) generating second digital signature keys and user's certificate;

d) setting an access authority of the file system;

e) identifying a user through a digital signature based authentication when the user tries to access the file system; and

f) giving the user the access authority for the file in accordance with identification result.

2. The method as recited in claim 1, further comprising the step of g) performing a user registering/deleting process if the user is identified as the system security manager.

3. The method as recited in claim 1, further comprising the step of h) setting the access authority of the file system if the user is identified as the system security manager.

4. The method as recited in claim 1, further comprising the step of i) accessing and processing a file.

5. The method as recited in claim 1, wherein the step a) includes the steps of:

a-1) generating a system security manager's public key;

a-2) generating a system security manager's secret key; and

a-3) generating system security manager's certificate.

6. The method as recited in claim 1, wherein the step e) includes the steps of:

e-1) generating, at a server computer, random numbers;

e-2) generating a digital signature to the random number;

e-3) extracting system security manager's public key from system security manager's certificate stored on the security kernel;

e-4) verifying user's certificate by system security manager's public key extracted;

e-5) extracting user's public key and the access authority in user's certificate; and

e-6) verifying the digital signature to the random number.

7. The method as recited in claim 1, wherein the step f) includes the steps of:

f-1) providing the user with the file system access authority to the file system if the user is the general user;

and

f-2) providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

8. The method as recited in claim 2, wherein the step g) includes the steps of:

g-1) determining whether user registration or deletion is selected;

g-2) deleting data related to a user to be deleted if the user deletion is selected;

g-3) registering a user if the user registration is selected;

wherein the step g-3) includes the steps of:

g-3-1) providing the user to be registered with the access authority;

g-3-2) generating a secret key and a public key of the user to be registered;

g-3-3) generating a certificate of the user to be registered;

g-3-4) encrypting and storing the secret key of the user to be registered; and

g-3-5) storing the certificate of the user to be registered.

9. The method as recited in claim 8, wherein the certificate is generated by encrypting the access authority

and user's public key.

10. The method as recited in claim 3, wherein the step h) includes the steps of:

h-1) selecting a file;

h-2) selecting a user allowed to be access the file; and

h-3) setting the access authority to the file as an access authority of the user.

11. The method as recited in claim 4, wherein the step i) accessing and processing a file includes the steps of:

i-1) receiving a name of a file to be accessed;

i-2) determining whether an access authority of the file to be accessed is equal to that of the system security manager;

i-3) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the system security manager;

i-4) determining whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

i-5) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user trying to access thereto.

12. An apparatus for protecting a file system in a computer system, wherein a user having a file access authority

can access the file system in the computer system, the method comprising:

means for generating system security manager's digital signature keys and system security manager's certificate;

means for storing system security manager's certificate onto a security kernel when installing an operating system on a server computer;

means for generating user's digital signature keys and user's certificate;

means for setting an access authority of the file system;

means for identifying a user through a digital signature authentication method when the user tries to access the file system; and

means for giving the user the access authority for the file in accordance with identification result.

13. The apparatus as recited in claim 12, further comprising means for performing a registration/deletion of the user if the user is identified as the system security manager.

14. The apparatus as recited in claim 12, further comprising means for setting the access authority of the file system if the user is identified as the system security manager.

15. The apparatus as recited in claim 12, further comprising means for accessing and processing a file.

16. The apparatus as recited in claim 12, wherein the means for generating system security manager's digital signature keys and system security manager's certificate includes:

means for generating system security manager's public key;

means for generating system security manager's secret key; and

means for generating system security manager's certificate.

17. The apparatus as recited in claim 12, wherein the means for identifying a user includes:

means for generating, at a server computer, random numbers;

means for generating a digital signature to the random number;

means for extracting system security manager's public key from in system security manager's certificate stored on the security kernel;

means for verifying user's certificate by system security manager's public key extracted;

means for extracting user's public key and the access authority in user's certificate; and

means for verifying the digital signature to the random number.

18. The apparatus as recited in claim 12, wherein the means for giving the user the access authority includes:

means for providing the user with the file system access authority to the file system if the user is the general user; and

means for providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

19. The apparatus as recited in claim 13, wherein the means for performing a registration/deletion of the user step g) includes:

means for determining whether user registration or deletion is selected;

means for deleting data related to a user to be deleted if the user deletion is selected;

means for registering a user if the user registration is selected;

wherein the means for registering a user includes:

means for providing the user to be registered with the access authority;

means for generating user's secret key and public key to be registered;

means for generating user's certificate to be registered;

means for encrypting and storing user's secret key to be registered; and

means for storing user's certificate to be registered.

20. The apparatus as recited in claim 19, wherein user's certificate is generated by encrypting the access authority of the user and user's public key.

21. The method as recited in claim 14, wherein the means for setting an access authority includes the steps of:

means for selecting a file;

means for selecting a user allowed to be access the file; and

means for setting the access authority to the file as an access authority of the user.

22. The method as recited in claim 15, wherein the means for accessing and processing a file includes:

means for receiving a name of a file to be accessed;

means for determining whether an access authority of the file to be accessed is equal to that of the security manager;

means for permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the security manager;

means for determining whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

means for permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user trying to access thereto.

23. A computer readable media storing instructions for executing a method for protecting a file system in a computer, wherein a user having an access authority for a file can access the file system in the computer, the method comprising the steps of:

a) generating system security manager's digital signature keys and system security manager's certificate;

b) storing system security manager's certificate onto a security kernel when installing an operating system on a server computer;

c) generating second digital signature keys and user's certificate;

d) setting an access authority of the file system;

e) identifying a user through a digital signature based authentication when the user tries to access the file system; and

f) giving the user the access authority for the file in accordance with identification result.

24. The computer readable media as recited in claim 23, wherein the method further comprises the step of g) performing a user registering/deleting process if the user is identified as the system security manager.

25. The computer readable media as recited in claim 23, wherein the method further comprises the step of h) setting the access authority of the file system if the user is

identified as the system security manager.

26. The computer readable media as recited in claim 23, wherein the method further comprises the step of i) accessing and processing a file.

27. The computer readable media as recited in claim 23, wherein the step a) includes the steps of:

a-1) generating a system security manager's public key;

a-2) generating a system security manager's secret key; and

a-3) generating system security manager's certificate.

28. The computer readable media as recited in claim 23, wherein the step e) includes the steps of:

e-1) generating, at a server computer, random numbers;

e-2) generating a digital signature to the random number;

e-3) extracting system security manager's public key from system security manager's certificate stored on the security kernel;

e-4) verifying user's certificate by system security manager's public key extracted;

e-5) extracting user's public key and the access authority in user's certificate; and

e-6) verifying the digital signature to the random number.

29. The computer readable media as recited in claim 23,

wherein the step f) includes the steps of:

f-1) providing the user with the file system access authority to the file system if the user is the general user; and

f-2) providing the user with registering/deleting authority, file system access setting authority and the file system access authority.

30. The method as recited in claim 24, wherein the step g) includes the steps of:

g-1) determining whether user registration or deletion is selected;

g-2) deleting data related to a user to be deleted if the user deletion is selected;

g-3) registering a user if the user registration is selected;

wherein the step g-3) includes the steps of:

g-3-1) providing the user to be registered with the access authority;

g-3-2) generating a secret key and a public key of the user to be registered;

g-3-3) generating a certificate of the user to be registered;

g-3-4) encrypting and storing the secret key of the user to be registered; and

g-3-5) storing the certificate of the user to be registered.

31. The computer readable media as recited in claim 30, wherein the certificate is generated by encrypting the access authority and user's public key.

32. The computer readable media as recited in claim 25, wherein the step h) includes the steps of:

h-1) selecting a file;

h-2) selecting a user allowed to be access the file; and

h-3) setting the access authority to the file as an access authority of the user.

33. The computer readable media as recited in claim 26, wherein the step i) accessing and processing a file includes the steps of:

i-1) receiving a name of a file to be accessed;

i-2) determining whether an access authority of the file to be accessed is equal to that of the system security manager;

i-3) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the system security manager;

i-4) determining whether the access authority of the file to be accessed is equal to that of the user trying to access thereto; and

i-5) permitting the file to be accessed if the access authority of the file to be accessed is equal to that of the user trying to access thereto.

FIG. 1

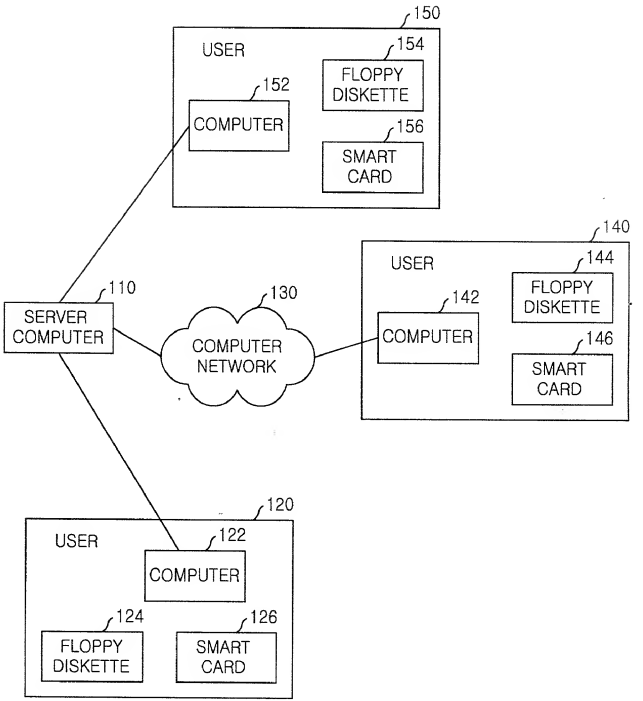

150
USER
154
FLOPPY DISKETTE
152
COMPUTER
156
SMART CARD
140
USER
144
FLOPPY DISKETTE
110
SERVER COMPUTER
130
COMPUTER NETWORK
142
COMPUTER
146
SMART CARD
120
USER
122
COMPUTER
124
FLOPPY DISKETTE
126
SMART CARD

FIG. 2

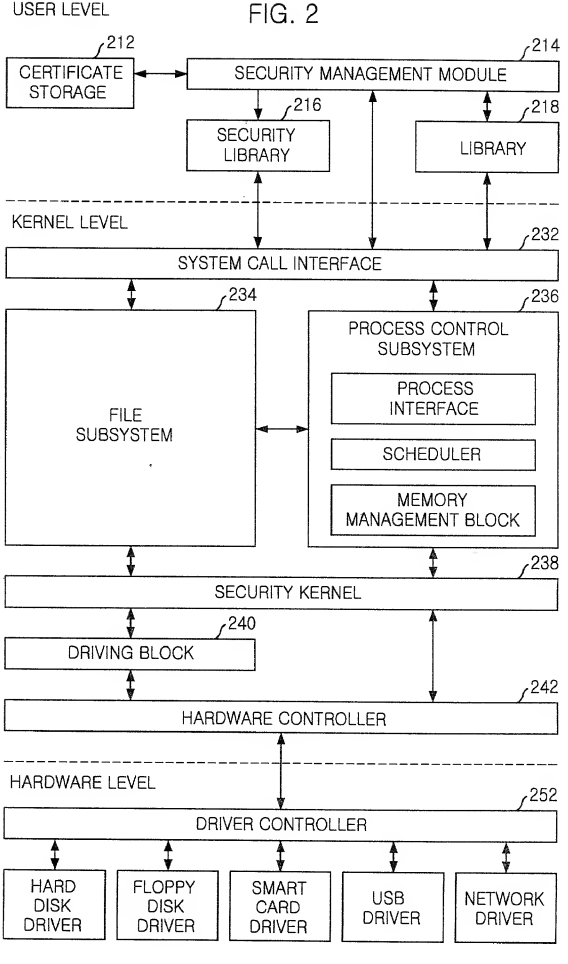

USER LEVEL
212
CERTIFICATE STORAGE
214
SECURITY MANAGEMENT MODULE
216
SECURITY LIBRARY
218
LIBRARY
KERNEL LEVEL
232
SYSTEM CALL INTERFACE
234
FILE SUBSYSTEM
236
PROCESS CONTROL SUBSYSTEM
PROCESS INTERFACE
SCHEDULER
MEMORY MANAGEMENT BLOCK
238
SECURITY KERNEL
240
DRIVING BLOCK
242
HARDWARE CONTROLLER
HARDWARE LEVEL
252
DRIVER CONTROLLER
HARD DISK DRIVER
FLOPPY DISK DRIVER
SMART CARD DRIVER
USB DRIVER
NETWORK DRIVER

FIG. 3

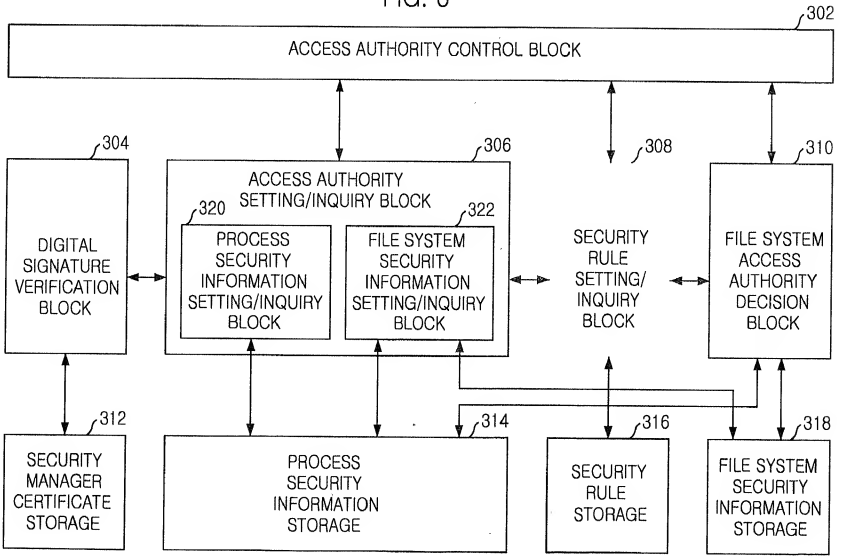


FIG. 4

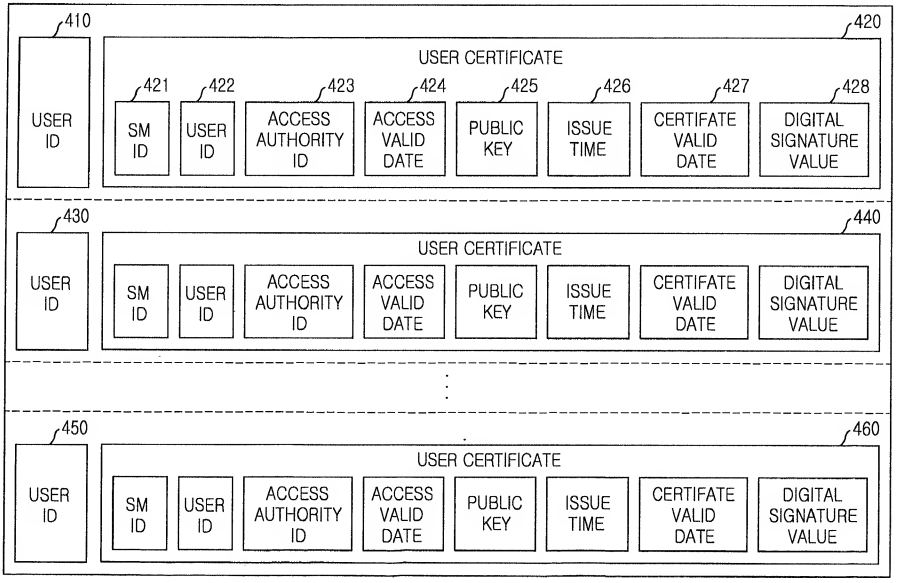


FIG. 5

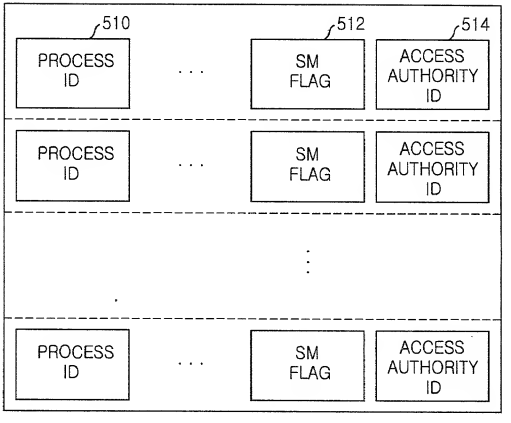

510
512
514
PROCESS ID
SM FLAG
ACCESS AUTHORITY ID
PROCESS ID
SM FLAG
ACCESS AUTHORITY ID
PROCESS ID
SM FLAG
ACCESS AUTHORITY ID

FIG. 6

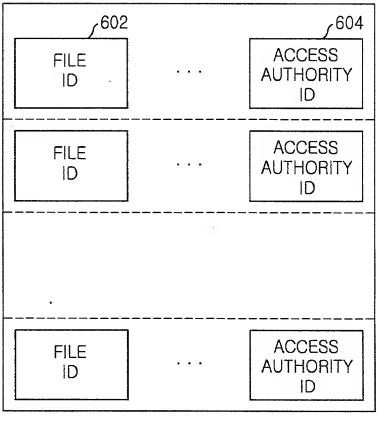

602
604
FILE ID
ACCESS AUTHORITY ID
FILE ID
ACCESS AUTHORITY ID
FILE ID
ACCESS AUTHORITY ID

FIG. 7

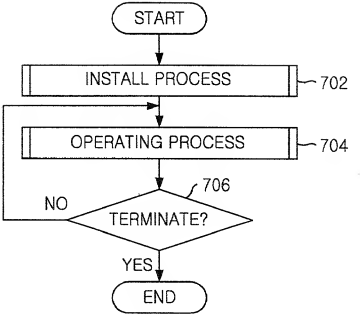

START
INSTALL PROCESS
702
OPERATING PROCESS
704
706
NO
TERMINATE?
YES
END

FIG. 8

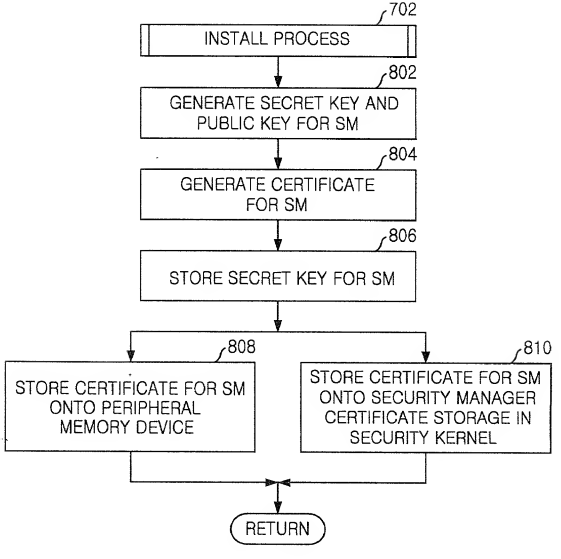

702
INSTALL PROCESS
802
GENERATE SECRET KEY AND PUBLIC KEY FOR SM
804
GENERATE CERTIFICATE FOR SM
806
STORE SECRET KEY FOR SM
808
STORE CERTIFICATE FOR SM ONTO PERIPHERAL MEMORY DEVICE
810
STORE CERTIFICATE FOR SM ONTO SECURITY MANAGER CERTIFICATE STORAGE IN SECURITY KERNEL
RETURN

FIG. 9

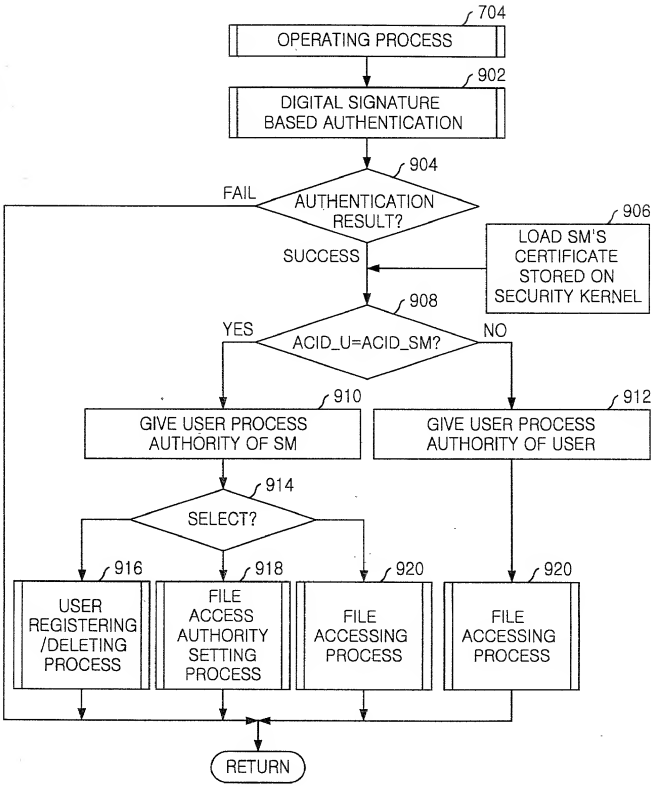

704
OPERATING PROCESS
902
DIGITAL SIGNATURE BASED AUTHENTICATION
904
AUTHENTICATION RESULT?
FAIL
SUCCESS
906
LOAD SM'S CERTIFICATE STORED ON SECURITY KERNEL
908
ACID_U=ACID_SM?
YES
NO
910
GIVE USER PROCESS AUTHORITY OF SM
912
GIVE USER PROCESS AUTHORITY OF USER
914
SELECT?
916
USER REGISTERING /DELETING PROCESS
918
FILE ACCESS AUTHORITY SETTING PROCESS
920
FILE ACCESSING PROCESS
920
FILE ACCESSING PROCESS
RETURN

FIG. 10

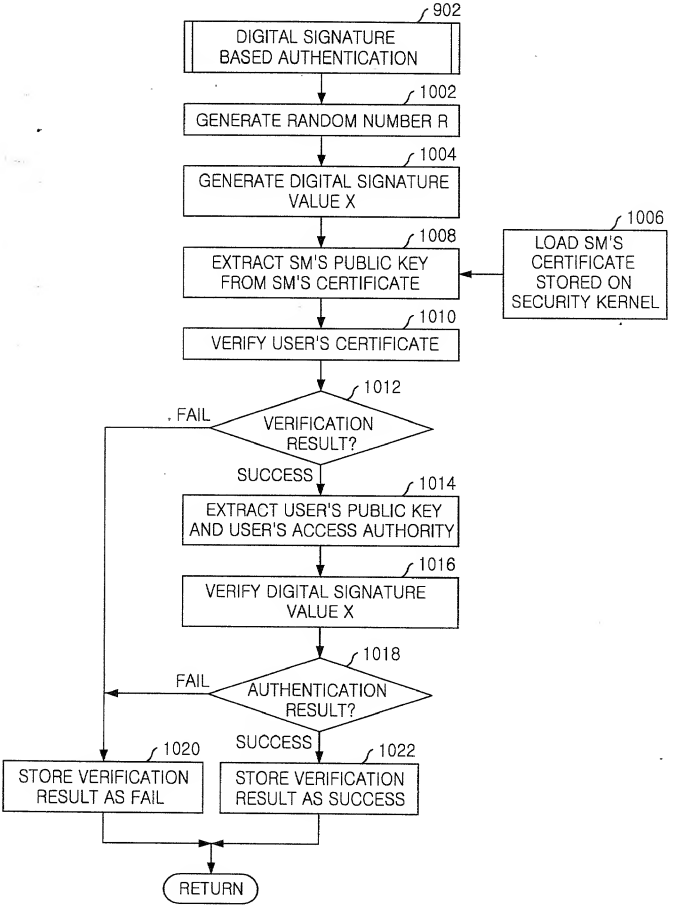

902
DIGITAL SIGNATURE BASED AUTHENTICATION
1002
GENERATE RANDOM NUMBER R
1004
GENERATE DIGITAL SIGNATURE VALUE X
1006
LOAD SM'S CERTIFICATE STORED ON SECURITY KERNEL
1008
EXTRACT SM'S PUBLIC KEY FROM SM'S CERTIFICATE
1010
VERIFY USER'S CERTIFICATE
1012
VERIFICATION RESULT?
FAIL
SUCCESS
1014
EXTRACT USER'S PUBLIC KEY AND USER'S ACCESS AUTHORITY
1016
VERIFY DIGITAL SIGNATURE VALUE X
1018
AUTHENTICATION RESULT?
FAIL
SUCCESS
1020
STORE VERIFICATION RESULT AS FAIL
1022
STORE VERIFICATION RESULT AS SUCCESS
RETURN

FIG. 11

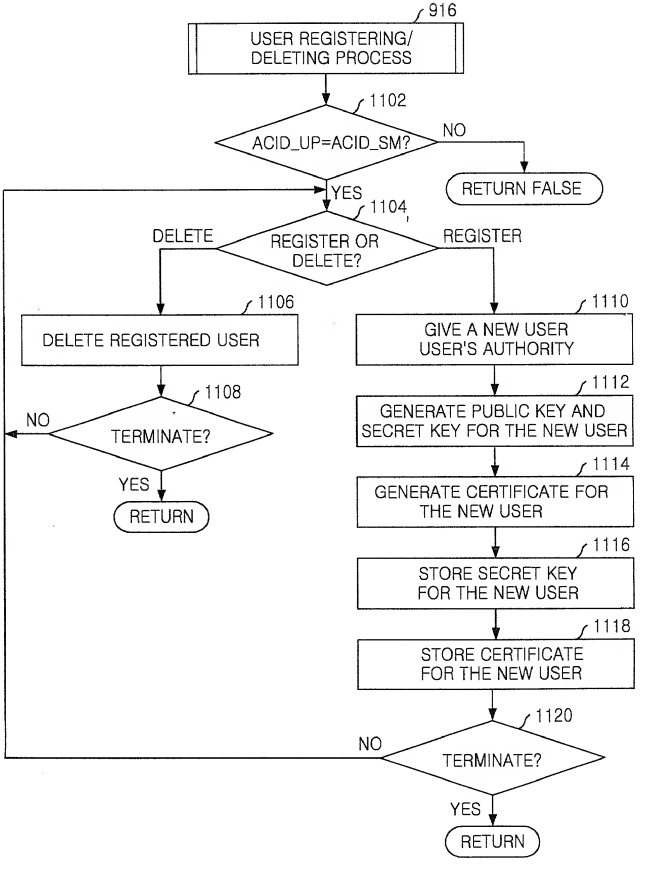

916
USER REGISTERING/ DELETING PROCESS
1102
ACID_UP=ACID_SM?
NO
RETURN FALSE
YES
1104
DELETE
REGISTER OR DELETE?
REGISTER
1106
DELETE REGISTERED USER
1108
NO
TERMINATE?
YES
RETURN
1110
GIVE A NEW USER USER'S AUTHORITY
1112
GENERATE PUBLIC KEY AND SECRET KEY FOR THE NEW USER
1114
GENERATE CERTIFICATE FOR THE NEW USER
1116
STORE SECRET KEY FOR THE NEW USER
1118
STORE CERTIFICATE FOR THE NEW USER
1120
NO
TERMINATE?
YES
RETURN

FIG. 12

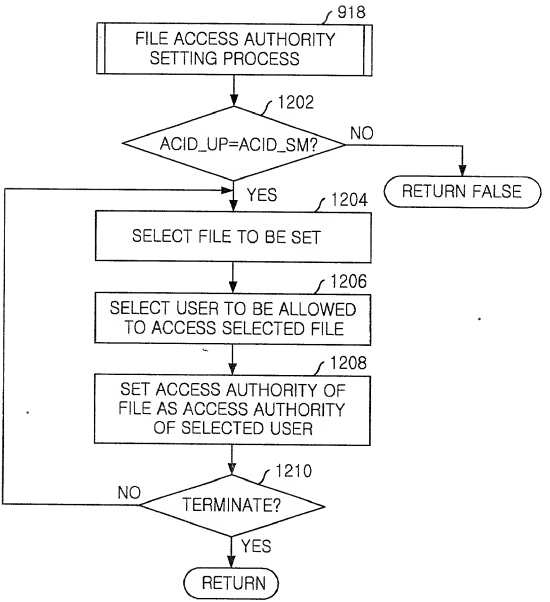
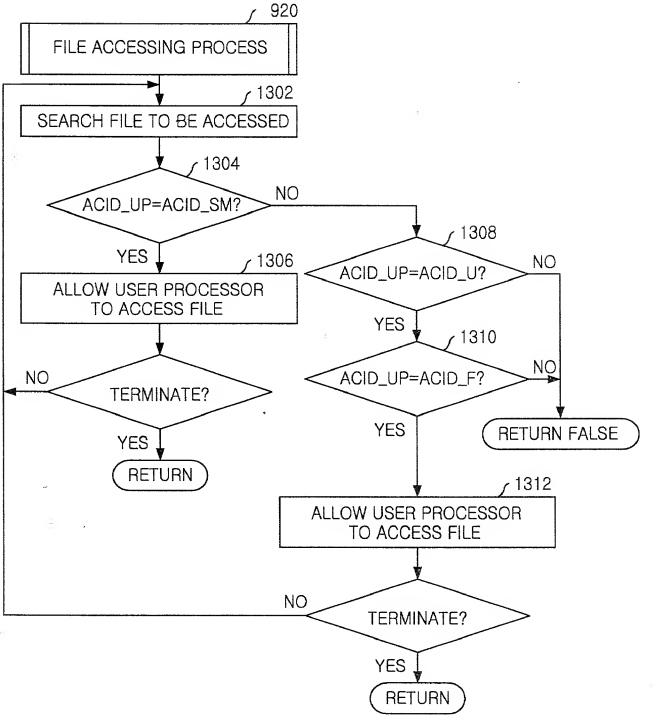

918
FILE ACCESS AUTHORITY SETTING PROCESS
1202
ACID_UP=ACID_SM?
NO
RETURN FALSE
YES
1204
SELECT FILE TO BE SET
1206
SELECT USER TO BE ALLOWED TO ACCESS SELECTED FILE
1208
SET ACCESS AUTHORITY OF FILE AS ACCESS AUTHORITY OF SELECTED USER
1210
NO
TERMINATE?
YES
RETURN

FIG. 13


920
FILE ACCESSING PROCESS
1302
SEARCH FILE TO BE ACCESSED
1304
ACID_UP=ACID_SM?
NO
YES
1306
ALLOW USER PROCESSOR TO ACCESS FILE
NO
TERMINATE?
YES
RETURN
1308
ACID_UP=ACID_U?
NO
YES
1310
ACID_UP=ACID_F?
NO
YES
RETURN FALSE
1312
ALLOW USER PROCESSOR TO ACCESS FILE
NO
TERMINATE?
YES
RETURN